公開

（事後評価・研究者用）

研　究　報　告　書

「デジタル回路設計における耐ハードウェアトロイ設計仕様の研究開発」

研究期間： 2018 年 10 月～2020 年 3 月
研究者番号： 50170
研 究 者： 大屋　優

1．　研究のねらい

近年、Integrated Circuit（IC）の設計・製造コスト削減のため、第三者に IC の設計・製造を委託している。そのため、第三者がハードウェアに悪意のある回路、いわゆるハードウェアトロイを挿入する危険性が問題視されている。設計工程におけるハードウェアトロイの脅威に対して、半導体のテスト手法を利用する研究が行われている。特にフォーマル検証によるテストを利用したハードウェアトロイ検出に関する研究開発が盛んである。フォーマル検証は IP の設計仕様と設計した回路が等価かどうかを確認する。

例えば、CPU の様に厳格な機能要求やバグによるセキュリティ違反のパターンに関するノウハウがある Intellectual Property（IP）なら、上記の要求を満たす設計仕様を作成することができ、フォーマル検証を用いることで安全性を検証することができる。しかしながら、半導体のセキュリティは近年問題視され始めてきた領域である。そのため、ノウハウの蓄積が不足しており、自社で設計した IP や他社の IP に対して、セキュリティを考慮した上で設計仕様を作成するのは困難である。これはハードウェアトロイの様にセキュリティを脅かす機能を持つ回路が含まれていることを仮定した上で検証することが、従来の観点では考えられてこなかった部分であり、検証可能な形で仕様に落とし込むことがうまくできないためである。

ハードウェアトロイ検出はフォーマル検証だけでは不十分であるということ以外にも直面している問題がある。それは、悪意のある機能をどのように判別すべきなのかという問題である。現在、危険だと疑われる箇所が特定されたとしても、それが仕様なのかバグなのか悪意のある機能なのかといった判別まで研究が進んでいない。この問題には、verification ではなく validation のアプローチを採用したテスト検証手法によって対応することが重要だと考えている。

最終的な研究の狙いは、日本で設計工程の IC の安全性を検証することができるようにすることである。日本の半導体事業が先細りの現状では、IP を設計するニーズが減っていき、専門的なエンジニアによる設計ノウハウが蓄積されにくい環境になってしまう。これでは、IP を外部から調達して IC を設計する際に、自社・自国で安全性を担保できなくなり、セキュリティ上の問題が生じた際に原因究明ができない可能性がある。本研究が少しでも、半導体のセキュリティが抱える問題の背景と今後対応していかなければならない問題への指針を示すことができれば幸いである。

2. 研究成果

（1）概要

まず、既存のハードウェアセキュリティ対策技術がハードウェアトロイに対してどの程度有効なのかを調査する実験を行い、対策できるハードウェアトロイと対策できないハードウェアトロイを明らかにすることができた。次に、対策できないハードウェアトロイを validation のアプローチでどの様に対策するのかを考察し、3 つの検証技術を研究開発した。開発した技術のコンセプトの正しさを検証するための、簡単な実験を行い、ハードウェアトロイの機能を違反として検出することに成功した。

1 つ目の、既存のハードウェアセキュリティ対策技術がハードウェアトロイに対してどの程度有効なのかを調査する実験について概説する。半導体の設計段階においてもセキュリティの重要性が高まっており、企業もセキュリティ対策技術の研究開発に着手している。現在、セキュリティ向けフォーマル検証の商用ツールにも採用されている、taint propagation 技術がある。そこで、まずは taint propagation 技術がハードウェアトロイ検出に対してどの程度有効なのかを検証することにした。実験対象のハードウェアトロイは、アメリカ国立科学財団が運営する Trust-HUB という Web サイトが公開されているベンチマークを使用した。ベンチマークは Register Transfer Level で記述されたハードウェアトロイが含まれており、ハードウェアトロイの機能はそれぞれ異なる。実験した結果、秘密鍵を漏洩するタイプのハードウェアトロイを検出することは確認できたが、それ以外のハードウェアトロイに対しては有効では無いということが判明した。ここで得られた実験結果とベンチマークを解析した知見を基に、既存の技術では対策できないハードウェアトロイを対象とした検証技術の研究開発に移った。

2 つ目の、対策できないハードウェアトロイを validation のアプローチでどの様に対策するのかを考察し、3 つの検証技術について概説する。検証手法には 3 つあり、ポートを検証する、データの値を検証する、アドレス参照を検証する、という 3 つである。アドレス参照に関しては実装できていない。そのためポートの検証、データの値の検証の 2 種類の検証技術が、taint propagation 技術では検出できないハードウェアトロイを検出することができることを、Trust-HUB ベンチマークを対象に実験することで確認した。

以上が本研究の概要である。

（2）詳細

研究テーマ「taint propagation 技術の調査」

既存のハードウェアセキュリティ対策のテスト検証技術として使われている taint propagation 技術のハードウェアトロイに対する有効性を調査する目的の実験を行なった。図 1 に taint propagation 技術のハードウェアトロイに対する有効性を調査する実験結果を示す。この実験で明らかになったのは、taint propagation 技術が元々フォーカスとしていた問題領域である、セキュアなデータがセキュアでない経路を通る性質のハードウェアトロイは無事に検出できていることである。そのため、taint propagation 技術によって対策が可能なハードウェアトロイは存在することは確認できた。この様な従来のハードウェアセキュリティの知見が強く活かせる暗号回路の様な分野では、極めて効果的だと考えられる。しかし、ハードウェアトロイは従来のハードウェアセキュリティで対応が難しい機能を持つ場合が多い。

それでは、taint propagation 技術が苦手とするハードウェアトロイはどんな性質を持ち、対応が困難な原因は何だろうか。taint propagation 技術は、データが移動する経路だけに着目する技術である。検査対象のデータに追跡用のタグの様なものを付加することで、使用者が検証して欲しいデータパスを *from a to b* の様な形で指定することで検証可能にする。検出可能な BasicRSA-T100 と BasicRSA-T300 では、秘密鍵が本来通るはずの経路を通らずに、バイパスしてプライマリアウトプットに接続されている。そのため、taint propagation 技術では、この秘密鍵のバイパス部分を違反として捉えることができ、結果的にハードウェアトロイを検出することにつながる。しかし、他のハードウェアトロイはデータパスが改竄されずに値だけが改竄される機能やある暗号化処理時の電力情報を意図的に偏らせる機能を持つため、検出が困難になる。

図 2 に taint propagation 技術がハードウェアトロイに対して有効でない原因を示す。図 2 で指摘する様にデータパスのみに着目するだけでは、データの不正な改竄、不正なアドレスの参照、余分なポートの追加、といった悪意のある改竄を検知することは難しい。そして、この様な機能こそがハードウェアトロイの肝となる機能となる。したがって、これらの機能に対する検証技術が必要であることが既存技術の調査を行なっていくことで判明した。

図 1. taint propagation 技術のハードウェアトロイに対する有効性を調査する実験結果

研究テーマ「研究すべき対象の機能と対応策」

図 3 に本研究技術が対象とするハードウェアトロイと検証技術の対応を示す。表の赤で塗られている行のベンチマークは taint propagation 技術で対策することが困難なハードウェアトロイを示す。表の右端に示す青で塗られた検証技術の列は、本研究で研究開発したどの検証技術で対策をするかの対応を示す。対応する検証技術は、ポートの検証、データの値の検証、アドレスの検証である。しかしながら、アドレスの検証に関しては実装を終えていないため、アプローチのコンセプトを説明するに留める。

まず、本研究の基本的なアプローチである validation 的なアプローチについて説明する。IP の検証は verification のアプローチによってテスト検証を行なっている。しかし、IP のセキュリティという観点による検証は一般的に行われておらず、CPU の様に研究や対策が進められている場合に限っては、セキュリティの検証も設計仕様に落とし込めるため verification で対策可能である。しかしながら、多くの IP ではセキュリティの専門家が不在であり設計仕様に落とし込むのは困難であり、verification で解決することには限界がある様に感じる。そこで、本研究では設計仕様に則って形式的検証を行うのではなく、テストエンジニアが怪しいと思った部分をテストエンジニアが検証できる様にサポートする方向性を目指している。本研究では設計データを読み込んで、ハードウェアトロイだと疑われる回路を解析し、自動的に怪しい箇所をピックアップする。そして、ハードウェアトロイか偽陽性の回路かを見分けるための、ハードウェアトロイらしい振る舞いの特徴と、その特徴を特定するためのアドバイスが表示される。

例えば、データの値の検証の場合、ハードウェアトロイは極めて低い確率の発火条件を設定し、定数で値を改竄する。そのため、ツールは極めて低い確率の発火条件を持つ回路部分をリストで表示する。テストエンジニアは、その条件が満たされた際に影響のある変数に対して、想定していた変数もしくはその変数が取るはずのない値を設定することで、ツール側がそのクエリを解析し違反するかどうかをチェックする。ツールはテストエンジニアが上記の様な手続きを可能にするために、予期せぬ値に改竄する機能を持つハードウェアトロイが存在することを教え、その場合にはどの様な変数に対してどの様なクエリを書くべきかもセットで示す。

ポートの検証では、想定しているモジュール間同士のポートを入力することで、接続忘れもしくは余計なポートの存在といった内容をチェックする。

アドレスの検証では、参照ビットを改竄する機能を持つハードウェアトロイがあるため、アドレス空間のマッピングが正しく行うことができるのかをチェックする。

以上が本研究の成果である。

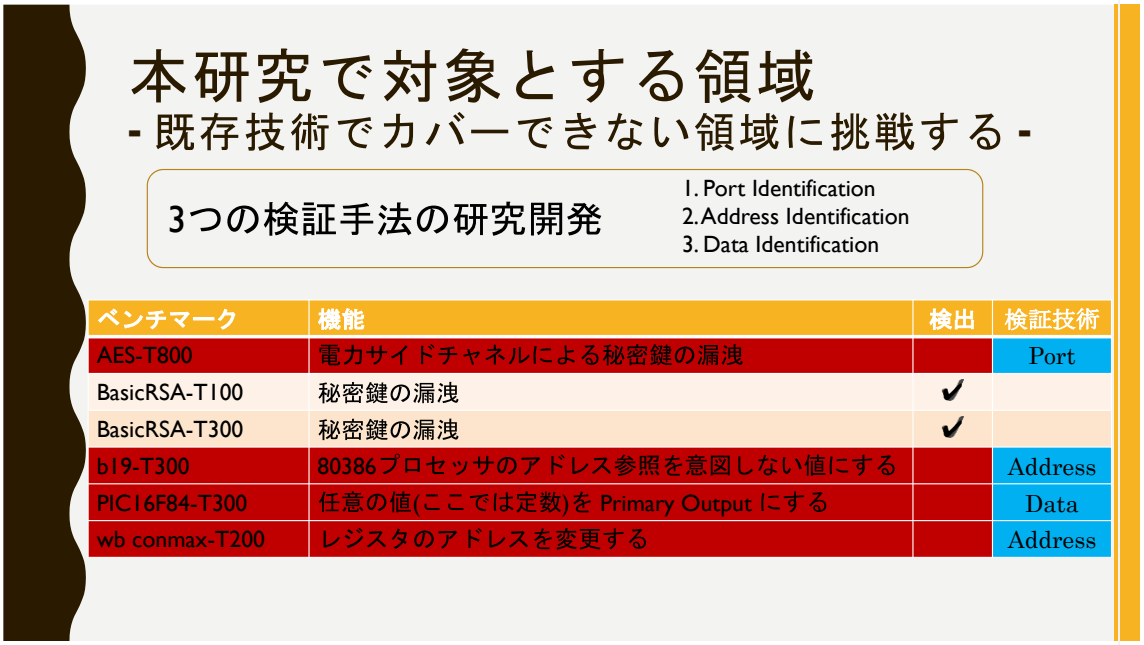

図 2.本研究技術が対象とするハードウェアトロイと検証技術の対応

3. 今後の展開

ハードウェアトロイについては多く研究者が危機意識を持ち、研究開発が世界中で行われているが、一般的な認知度は低い。しかしながら、いつかのタイミングで対策を講じる必要はあるのではないかと判断し、情報の収集を行う産業界のエンジニアも多い。そのため、今後は産業界から本研究分野に対して動きが加速していくものと思われる。本研究の成果ではないが、実際に私の研究内容が産業界で実製品化され、半導体の検証サービスの一工程という位置付けのセキュリティ検証サービスで使用されることが決定されている。本研究も私自身のこれまでの研究の様に社会実装に至るまで質を高めていくつもりである。方針としては、ハードウェアトロイの検出における verification アプローチの有効範囲を明らかにすることと、validation アプローチの有効性の確認が急務である。特に validation アプローチをとるにあたって、エンジニアが受け持つ役割と研究開発する技術が受け持つ役割を明らかにしなければならない。ハードウェアトロイであると判断するためにエンジニアが持つ前提知識に応じて、エンジニアが入力することができるパラメータの有無が異なるため、解析のために手法に用いることができるパラメータも異なるためである。今後も実用性と妥当性を兼ね備えることのできるパラメータの選出に関して考察を進めていく。研究の世界だけを向くのではなく、研究室の外を見据えた研究を行うことで、本研究がハードウェアトロイ研究に対する産業界からの理解や興味が深まる一助となることを望む。

また、長期的な展望としては最終的にハードウェアトロイかどうかといったノウハウが蓄積されていくことにより、セキュリティという観点を設計仕様に落とし込むことができ、フォーマル検証の様な verification でも対応できるケースが増えていくと考えている。

研究自体ではないが、他にも重要な問題として、ハードウェアトロイの周知が挙げられる。私自身、今までハードウェアトロイに関する周知活動としては、大手 EDA ツールの企業が開催するユーザカンファレンスで招待講演や、CEATEC 2019 での展示等をしたが、ネットワークやアプリのセキュリティ程の認知度は得られていないと感じる。今後もハードウェアトロイの問題に関する情報の発信に努めたい。

4. 自己評価

ハードウェアトロイを検出することのできる設計仕様の作成を目的としていたが、テスト対象の IP の完全な設計仕様があるという理想的な状態を仮定しないと、フォーマル検証でハードウェアトロイを検出することは現実的でないことが判明した。そこで、異なるアプローチとして validation を意識した検証手法の研究開発に舵を切った。これはハードウェアトロイと疑われた回路の場所が与えられた場合、“どの情報”を“どの様な手法”でハードウェアトロイと判断できるかという問題である。従来のハードウェアトロイ検出はハードウェアトロイと疑われる候補を検出することに注力しており、候補を検出した後にどうするかといった手法には着目していなかった。しかし、実際にハードウェアトロイ検出手法を運用するためには、候補の検出は一工程に過ぎず、偽陽性と偽陰性の区別が不可欠である。そこで、本研究ではハードウェアトロイ候補が与えられた場合に、実際にどの様な手続きを経てハードウェアトロイと判断すべきなのかという点に注目し研究開発に着手した。研究の方針の転換はあったものの、ハードウェアトロイの仕込まれたベンチマークの解析は、研究の方針の如何に関わらず有用だった。

この解析により、どの様なタイプのハードウェアトロイだと、どの情報に着目するだけで検出できるのかを明らかにすることができ、ハードウェアトロイと判断する手法の開発に役立った。

また、種々の実験を通じて、フォーマル検証の苦手な部分や商用ツールで対応できない点を明確にすることができた。これにより、広く半導体のテスト検証に使われるフォーマル検証に従事しているエンジニアに対して、ハードウェアトロイを考える際に現在のツールで何をカバーして、足りない部分は本研究を含めてどの様なアプローチで対応すべきなのかといったことを訴求していくことができる。特に新しい問題に対して、従来手法と新手法の持つ機能の責任を切り分けることは、新しいことを提案する際に非常に重要なことだと考える。本研究を通じて、ハードウェアトロイ検出を取り巻く議論の下地の整備をすることができたのは大きい。これにより、半導体検証というバックグラウンドを持つ企業で働くエンジニアに対しても、彼らのバックグラウンドに合わせて説明を行うことができる様になり、より深くハードウェアトロイという問題に対して理解を深めることに繋がると思われる。

5. 主な研究成果リスト

(1)論文(原著論文)発表

特に無し。

(2)特許出願

研究期間累積件数:0件

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

大屋優, “設計から切り込む IoT セキュリティ, ”CEATEC 2019, 千葉県千葉市幕張メッセ, 2019 年 10 月 15 日—2019 年 10 月 18 日.